REMARKS

Reconsideration of the rejections set forth in the Office Action dated September 20, 2006 is respectfully requested. By this amendment claims 8 and 12 have been canceled without prejudice or disclaimer, and claims 1-3, 7, 10, 14-16, and 21 have been amended. Currently, claims 1-7, 9-11, and 13-25 are pending in this application.

Rejection under 35 USC 102

Claims 1-10, 12-18, 20, and 22-25 were rejected under 35 USC 102 as anticipated by Baker (U.S. Patent No. 7,035,898). This rejection is respectfully traversed in view of the amendments to the claims and the following arguments.

This application relates to industrial networks, and more particularly to a way in which access to particular PLCs and attendant factory machines may be circumscribed so that only particular authorized individuals may have access to particular PLCs. As discussed in the background of the specification, for example at page 1, PLCs are able to be connected to a company's Ethernet network or other data network. However, where there is more than one person that is allowed to program PLCs on the network, a person may accidentally make a change to the wrong PLC or a person may intentionally change the programs of PLCs on the network to affect operation of the machines associated with the PLCs. As described at page 9, line 27 to page 10, line 6, the SPIP is configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel. This enables unauthorized individuals from viewing and/or modifying the communications between the SPIP and the central control or other network devices, and also enables other sundry benefits attendant to VPNs to be implemented in connection with programming PLCs.

Baker teaches a way in which a remote HMI may be used to program PLCs over the Internet. In particular, Baker teaches a web server that may be accessed via the Internet. When the user first accesses the web server 30, the web server will provide a home page for a website 4. The website 4 includes a network interface 16 which includes the IP address 18 and a firewall or security. Once the user has gotten past the firewall the user is able to interact with a programming device 21 that may be used to modify application programs 22. Thus, Baker teaches a central programming facility, which is web based, and which may be used to adjust

PLC code from anywhere on the network. Access to the web site is controlled in Baker by including a password and user list in the initial configuration files for the web-site. (see Col. 5, lines 22-26). In connection with Fig. 5, Baker teaches that some or all of the components of the web site may reside on the PLC. However, Baker does not teach or suggest implementing a VPN to access the web site to secure communications with the PLC.

Applicants have amended the claims to recite a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel.

Claim 21 previously recited that the SPIP included a virtual private network module configured to participate in a virtual private network tunnel established on the industrial network. This claim was not rejected under 35 USC 102 over Baker and, accordingly, applicants respectfully submit that the claims as amended are not anticipated by Baker. Accordingly, applicants respectfully request that the rejection under 35 USC 102 be withdrawn.

Claim 21 was rejected, however, over a combination of Baker and Tilton (U.S. Patent Application Publication No. 2004/0068562). Specifically, the Examiner has taken the position that Tilton teaches the use of a Virtual Private Network. (Although paragraph 30 of the Office Action refers to Baker, the actual citation is to portions of Tilton. Accordingly, applicants have treated this rejection as referring to Tilton).

Tilton teaches that accessing a resource such as a server or other active device may expose the server/active device to viruses and other vulnerabilities. (Par. 2). Thus, Tilton seeks to restrict access from an active device to other resources on the network (Par. 3). With this background, Tilton teaches a system (service station) that determines whether a requesting device is properly configured before allowing the requesting device to access an active device. If the requesting device is not properly configured, the service station will cause a router to block access to the active device.

With respect to claim 21, the Examiner cited paragraph 47 and Fig. 1, #30 of Tilton as teaching a VPN. Item 30a is identified in Fig. 1 as a VPN Microsoft Client, and item 30b is identified in Fig. 1 as a VPN non-Microsoft client. These VPN clients are described in paragraph 16 as being the requesting clients that are seeking access to the active device, such as server 40. Paragraph 47, cited by the Examiner, describes how different severity levels of non-compliance with a particular set of rules may be used to determine what type of access the clients should get to the private network and/or the active device.

Tilton does not address programmable logic controllers or industrial networks, and does not appear to be otherwise relate to the technology involved in this application. Rather, the only tenuous connection is that Tilton happens to show a Microsoft VPN client, which is a common client that may be used to access a local area network from a remote location. Tilton does not teach or suggest implementing a VPN with a PLC or otherwise teach or suggest that a VPN may be implemented as claimed in the claims as amended. Rather Tilton merely teaches a Microsoft VPN client implemented on a personal computer that is attempting to connect to a local area network or to a server.

Accordingly, applicants respectfully submit that the combination of Tilton and Baker would not have taught or suggested a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel.

Moreover, applicants additionally respectfully submit that there is no motivation to combine Baker with Tilton. Applicants have not discerned why a person of ordinary skill in the art would have been motivated to combine the teachings of these two references. Additionally, the rejection of claim 21 does not specify any such motivation to combine, which is an essential piece of an obviousness rejection. Accordingly, applicants respectfully submit that it would not have been obvious to select these two references and also respectfully submit that the Examiner has failed to set forth, prima facie, that it would have been obvious to do so. For these additional reasons, applicants respectfully submit that the claims as amended are patentable over the cited art.

Conclusion

In view of foregoing remarks, it is respectfully submitted that the application is now in condition for allowance and an action to this effect is respectfully requested. If there are any questions or concerns regarding the amendments or these remarks, the Examiner is requested to telephone the undersigned at the telephone number listed below.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-15929).

Respectfully Submitted

John C. Gorecki

Dated: February 6, 2007

John C. Gorecki
Registration No. 38,471

John C. Gorecki, Esq.
P.O. Box 553
Carlisle, MA 01741
Tel: (978) 371-3218
Fax: (978) 371-3219
john@gorecki.us